ИНФОРМАТИКА

2008 **январь-март** **№ 1**

УДК 004.9

А.А. Коляда, В.В. Ревинский, А.Ф. Чернявский, Е.В. Шабинская

ЧЕТЫРЕХМОДУЛЬНАЯ СИСТЕМА ОБРАБОТКИ ИНФОРМАЦИИ ДЛЯ ВЫСОКОТОЧНЫХ ВЫЧИСЛЕНИЙ

Разрабатывается методология синтеза немодульных процедур для высокоточных систем модулярной обработки информации (СМОИ), функционирующих в режиме модульных вычислений (РМВ). Ее основу составляет новый метод – метод доминирующего модуля. В рамках минимально избыточного модулярного кодирования предложенный подход позволяет уменьшить сложность базовой немодульной операции до O(k) таблиц (k – число модулей используемой системы счисления). Развиваемая технология построения РМВ-СМОИ на базе минимально избыточной модулярной арифметики демонстрируется на примере четырехмодульной системы, которая адаптирована к приложениям в цифровой обработке сигналов.

Введение

В современных приложениях модулярной арифметики особое место занимают разработки по созданию высокопроизводительных параллельных систем, которые полностью функционируют в так называемом режиме модульных вычислений [1–11]. Данный режим характеризуется отсутствием округлений на модульных сегментах вычислительных процессов, т. е. на сегментах, состоящих только из модульных операций: сложения, вычитания и умножения в модулярной системе счисления (МСС) без контроля переполнения. При этом предполагается, что результаты счета на каждом модульном сегменте не выходят за пределы используемого динамического диапазона. Таким образом, его мощность, по крайней мере, должна превосходить квадраты элементов диапазона исходных данных МСС. Так как модульные операции в модулярном коде выполняются поразрядно, т. е. независимо по каждому из модулей, то в рамках РМВ наряду с отсутствием округлений благодаря параллельной природе модулярной арифметики достигается высокая производительность.

Как отмеченное, так и ряд других фундаментальных преимуществ модулярных вычислительных структур идеально согласуются с реализационными принципами передовых компьютерных технологий параллельной обработки информации, таких, в частности, как мультипроцессорная, нейронносетевая технологии и др. [3, 9–14].

В последние годы СМОИ все шире применяются для проведения высокоточных и абсолютно точных вычислений. Прежде всего это относится к приложениям в области цифровой обработки сигналов, распознавания образов и обработки изображений, а также защиты информации. В настоящее время среди систем указанного класса приоритетные позиции занимают СМОИ, которые реализуются программными способами (без использования специальных аппаратных средств). В рамках существующих и интенсивно развивающихся компьютерных технологий параллельной обработки возможности для организации на программном уровне РМВ и увеличения пределов его действия неуклонно расширяются.

Вполне понятно, что расширение пределов действия РМВ сопряжено с ростом значений результирующих переменных на модульных сегментах, а следовательно, и мощности требуемого динамического диапазона. Для предотвращения выхода результатов счета за границы диапазона в СМОИ обычно применяются операции масштабирования или другие немодульные операции. Например, в системах криптографической защиты информации роль такой операции выполняет операция приведения элементов динамического диапазона МСС к остаткам по большим простым модулям. Эффективной компьютерно-арифметической базой для решения проблемы немодульных процедур является минимально избыточная модулярная арифметика (МИМА) [1, 9–11, 15, 16].

Настоящая статья посвящена проблематике построения на основе МИМА высокоточных СМОИ, функционирующих в РМВ. Предлагаемые подходы демонстрируются на примере четырехмодульной МИМА-СМОИ, которая адаптирована к практическим применениям.

1. Минимально избыточные МСС

В множестве **Z** целых чисел минимально избыточная МСС (МИМСС) определяется с помощью $k>1$ попарно простых основных модулей $m_1, m_2,\ldots, m_k$ и вспомогательного модуля m_0, удовлетворяющего условиям $(m_i, m_0)=1$ $(i=\overline{1,k})$ и $m_k > 2m_0$. При этом в качестве рабочего диапазона используется множество

$$\boldsymbol{D} = \mathbf{Z}_{2M}^{-} = \{-M,\ -M+1,\ ...,\ M-1\} \quad \left(M=m_0M_{k-1}; M_{k-1}=\prod_{i=1}^{k-1} m_i \right).$$

Число $X \in \boldsymbol{D}$ в МИМСС представляется модулярным кодом

$$(\chi_1, \chi_2,..., \chi_k) \in \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times ... \times \mathbf{Z}_{m_k},\ \chi_i = \left| X \right|_{m_i};$$

через $\left| a \right|_m$ обозначается элемент из кольца вычетов $\mathbf{Z}_m = \{0, 1, ..., m-1\}$, сравнимый с величиной a (в общем случае рациональным числом) по натуральному модулю m.

Как и в обычной МСС с основаниями $m_1, m_2, \ldots, m_k$, кольцевые операции над произвольными целыми числами (ЦЧ) A и B, заданными своими модулярными кодами

$$A = (\alpha_1,\alpha_2,...,\alpha_k),\ B=(\beta_1,\beta_2,...,\beta_k)\ (\alpha_i = \left|A\right|_{m_i},\ \beta_i = \left|B\right|_{m_i}\ (i=\overline{1,\ k})),$$

в МИМСС выполняются независимо по каждому из модулей, т. е. по правилу

$$\begin{gathered} A \circ B = (\alpha_1,\alpha_2,...,\alpha_k) \circ (\beta_1,\beta_2,...,\beta_k) = \\ = (|\ \alpha_1 \circ \beta_1\ |_{m_1},\ |\ \alpha_2 \circ \beta_2\ |_{m_2},...,\ |\ \alpha_k \circ \beta_k\ |_{m_k})\ \ (\circ \in \{+, -, \times\}). \end{gathered} \tag{1}$$

Именно в свойстве (1) модулярной арифметики и заключается ее главное фундаментальное преимущество над арифметикой позиционных систем счисления.

Восстановление числа $X \in \boldsymbol{D}$ по его коду $(\chi_1, \chi_2,..., \chi_k)$ в МИМСС осуществляется с помощью так называемого интервального индекса (ИИ) $I(X)$ и определяющей его интервально-модулярные формы (ИМФ) числа X, которая имеет вид

$$X = \sum_{i=1}^{k-1} M_{i,k-1} \left| M_{i,k-1}^{-1} \chi_i \right|_{m_i} + M_{k-1} I(X)\ \ (M_{i,k-1}^{-1} = M_{k-1}\ /\ m_i). \tag{2}$$

Согласно китайской теореме об остатках (КТО) интервально-индексная характеристика $I(X)$ модулярного кода $(\chi_1, \chi_2,..., \chi_k)$ соотношением (2) определяется однозначно [1, 15].

Сущность принципа минимально избыточного модулярного кодирования раскрывается следующей теоремой [15].

Теорема 1. *Для того чтобы в МСС с попарно простыми основаниями $m_1, m_2, \ldots, m_k$ ($k>1$) ИИ $I(X)$ каждого элемента X диапазона $\boldsymbol{D} = \mathbf{Z}_{2M}^{-} = \{-M, -M+1, ..., M-1\}$ полностью определялся вычетом $\hat{I}_k(X) = \left|I(X)\right|_{m_k}$, необходимо и достаточно, чтобы k-е основание МСС удовлетворяло условию $m_k \geq 2\ m_0 + \rho$, где m_0 – вспомогательный модуль, взаимно простой с $m_1, m_2, ..., m_k$; $\rho = max\{\rho_{k-1}(X)\}$; $\rho_{k-1}(X)$ – интегральная характеристика модулярного кода (ИХМК), определяемая равенством*

$$\left| X \right|_{M_{k-1}} = \sum_{i=1}^{k-1} M_{i,k-1} \left| M_{i,k-1}^{-1} \chi_i \right|_{m_i} - M_{k-1} \rho_{k-1}(X) \quad (\chi_i = \left| X \right|_{m_i}). \tag{3}$$

При этом для $I(X)$ верны расчетные соотношения

$$I(X) = \begin{cases} \hat{I}_k(X), & \text{если } \hat{I}_k(X) < m_0; \\ \hat{I}_k(X) - m_r, & \text{если } \hat{I}_k(X) \geq m_k - m_0 - \rho; \end{cases} \tag{4}$$

$$\hat{I}_k(X) = \left| \sum_{i=1}^{k} R_{i,k}(\chi_i) \right|_{m_k}; \tag{5}$$

$$R_{i,k}(\chi_i) = \left| -m_i^{-1} \left| M_{i,k-1}^{-1} \chi_i \right|_{m_i} \right|_{m_k} \quad (i \neq k), \quad R_{k,k}(\chi_k) = \left| \frac{\chi_k}{M_{k-1}} \right|_{m_k}. \tag{6}$$

Очевидно, МСС с модулями m_1, m_2, ..., m_k и диапазоном $\boldsymbol{D}$, выбираемыми в соответствии с теоремой 1, имеет наименьшую избыточность, когда выполняется равенство $m_k - 2m_0 - \rho = \left| m_k - \rho \right|_2$. Именно в этом случае МСС называется минимально избыточной.

Приведем численный пример.

Пример 1. Рассмотрим трехмодульную МИМСС с основными модулями m_1=2, m_2 =3, m_3 =11. Из (3) вытекает равенство $\rho_{k-1}(X) \left\lfloor \sum_{i=1}^{k-1} m_i^{-1} \left| M_{i,k-1}^{-1} \chi_i \right|_{m_i} \right\rfloor$ (через $\lfloor a \rfloor$ обозначается целая часть величины a). Следовательно, для заданной МИМСС $\rho = \lfloor (1/2) + (2/3) \rfloor = 1$ согласно теореме 1 наименьшая избыточность обеспечивается при вспомогательном модуле m_0 =5. В этом случае достигается равенство $m_3 = 2m_0 + \rho$.

Константы ИМФ (2) принимают значения $M_{k-1} = M_2 = 2 \cdot 3 = 6$; $M_{1,\,k-1} = M_{1,2} = M_2 / m_1 = 6/2 = 3$; $M_{2,\,k-1} = M_2 / m_2 = 6/3 = 2$; $\left| M_{1,k-1}^{-1} \right|_{m_1} = \left| 1/3 \right|_2 = 1$; $\left| M_{2,k-1}^{-1} \right|_{m_2} = \left| 1/2 \right|_3 = 2$. Таким образом, выражение (2) имеет вид

$$X = 3\chi_1 + 2\left| 2\chi_2 \right|_3 + 6I(X).$$

Для вычисления $I(X)$ по (4)–(6) обычно применяются таблицы, в которых хранятся значения вычетов (6). В данном случае $\left| -m_1^{-1} \right|_{m_k} = \left| -1/2 \right|_{11} = 5$; $\left| -m_2^{-1} \right|_{m_k} = \left| -1/3 \right|_{11} = 7$; $\left| M_{k-1}^{-1} \right|_{m_k} = \left| 1/6 \right|_{11} = 2$. Поэтому, как показывают расчеты по формулам (6), искомые таблицы ИИ имеют вид

$$\text{ТИ1} = \left\{ R_{1,3}(\chi_1) \right\} = \{0,5\}; \; \text{ТИ2} = \left\{ R_{2,3}(\chi_2) \right\} = \{0, 3, 7\};$$

$$\text{ТИ3} = \left\{ R_{3,3}(\chi_3) \right\} = \{0, 2, 4, 6, 8, 10, 1, 3, 5, 7, 9\}.$$

Ввиду $M = \prod_{i=0}^{2} m_i = 5 \cdot 2 \cdot 3 = 30$ диапазоном рассматриваемой МИМСС служит множество $\boldsymbol{D}$={–30, –29, …, 29}.

Пусть в МИМСС задано число с модулярным кодом (χ_1, χ_2, χ_3)=(1,2,7). Применяя соотношение (5), находим: $\hat{I}_3(X) = \left|TII1[1] + TII2[2] + TII3[7]\right|_{11} = \left|5 + 7 + 3\right|_{11} = 4$. Поскольку $\hat{I}_3(X) = 4 < m_0 = 5$, то согласно (4) $I(X) = \hat{I}_3(X) = 4$. Таким образом, в соответствии с приведенной выше ИМФ заданному коду отвечает число X=3·1+2·1+6·4=29. Проверка показывает, что число 29 действительно имеет модулярный код (1,2,7).

Для неизбыточной МСС с основаниями m_1, m_2, ..., m_k и диапазоном $\mathbf{Z}_{M_k}$ КТО можно записать в виде

$$X = \left| \sum_{i=1}^{k} M_{i,k} \left| M_{i,k-1}^{-1} \chi_i \right|_{m_i} \right|_{M_k}.$$

Отсюда видно, что непосредственное применение КТО для синтеза процедур модулярной арифметики неприемлемо, по крайней мере, по следующим причинам. Компьютерная реализация приведенного выражения требует операции взятия вычета по большим модулям. Данная операция весьма трудоемка, особенно при работе в диапазонах большой мощности. Кроме того, КТО не приспособлена для оперирования над элементами симметричных диапазонов и непригодна для построения процедур масштабирования. От указанных недостатков ИМФ свободна.

2. Метод доминирующего модуля для выполнения немодульных операций в МИМСС

Важнейшее достоинство СМОИ, полностью функционирующих в РМВ, заключается в том, что эти системы требуют минимального алгоритмического обеспечения. В его состав, как правило, достаточно включить процедуры выполнения модульных операций, а также прямого и обратного преобразований, чаще всего с масштабированием позиционного и модулярного кодов. Поскольку входные кодовые преобразования, т. е. преобразования позиционных кодов в модулярные коды, существенных затруднений не вызывают, то главное внимание в данном разделе уделяется проблематике синтеза процедур выходного кодового преобразования с масштабированием.

Как следует из теоремы 1, в ее условиях расчет интервально-индексной характеристики $I(X)$ согласно (4)–(6) фактически сводится к суммированию k вычетов по модулю m_k, т. е. является тривиальной операцией. Для вычисления традиционно применяемых интегральных характеристик модулярного кода (цифр полиадического кода, ранговой характеристики и других) необходимо выполнить суммирования по модулям МСС k наборов вычетов. Использование МИМСС вместо МСС снижает сложность алгоритма формирования базовой характеристики, выражаемую количеством необходимых таблиц и числом сложений по модулям, с $O(k^2)$ до $O(k)$. Исходя из сказанного в качестве основы для синтеза немодульных процедур для РМВ-СМОИ, естественно, целесообразно принять ИМФ (2) и соотношения (4)–(6) для расчета ИИ.

Остановимся подробнее на операции выходного кодового преобразования, которое состоит в получении по минимально избыточному модулярному коду $(\chi_1, \chi_2, ..., \chi_k)$ произвольного $X \in \boldsymbol{D}$ его позиционного кода. Как уже отмечалось, данную операцию в РМВ-СМОИ ввиду большой мощности динамического диапазона $\boldsymbol{D}$ чаще всего приходится осуществлять с масштабированием. Таким образом, задача заключается в формировании позиционного кода некоторой целочисленной оценки $\hat{X}$ дроби $x = X/S$, где S – выбранный масштаб.

При использовании сверхбольшого модуля ИИ вида $m_k = 2^{b_k}$ (b_k – натуральное число) для выполнения указанной операции выходного кодового преобразования удается разработать исключительно простой и эффективный метод, который назван методом доминирующего модуля. Его основу составляет следующая теорема.

Теорема 2. *Пусть масштабирующий множитель* S *имеет вид*

$$S = sM_{k-1}\ (s \geq 2k-2). \tag{7}$$

Тогда в МИМСС с основаниями $m_1, m_2, \ldots, m_k$ *и динамическим диапазоном* $\boldsymbol{D}$ *дробь* $x=X/S$ $(X \in \boldsymbol{D})$ *может быть аппроксимирована целочисленной величиной*

$$\hat{X} = \lfloor I(X)/s \rfloor, \tag{8}$$

где $\lfloor a \rfloor$ *– ближайшее к вещественной величине* a *ЦЧ*:

$$\lfloor a \rfloor = \begin{cases} \lfloor a \rfloor, & \text{если } a < \lfloor a \rfloor + 0{,}5, \\ \lceil a \rceil, & \text{если } a \geq \lfloor a \rfloor + 0{,}5; \end{cases}$$

$\lfloor a \rfloor$ *– целая часть вещественной величины* a, $\lceil a \rceil$ *– наименьшее ЦЧ, не меньшее* a. *При этом аппроксимация* (8) *обладает абсолютной погрешностью* $\left| x - \hat{X} \right| < 1$.

Доказательство. Вычитая и добавляя в правой части ИМФ (2) величину $M_{k-1}\rho_{k-1}(X)$ и применяя затем (3), получим

$$\begin{aligned} X = \sum_{i=1}^{k-1} M_{i,\,k-1} \left| M_{i,\,k-1}^{-1}\ \chi_i \right|_{m_i} - M_{k-1}\rho_{k-1}(X) + M_{k-1}\rho_{k-1}(X) + M_{k-1}I(X) = \\ = \left| X \right|_{M_{k-1}} + M_{k-1}\rho_{k-1}(X) + M_{k-1}I(X). \end{aligned} \tag{9}$$

Применяя симметрическую версию леммы Евклида [15], представим $I(X)$ в виде

$$I(X) = \left| I(X) \right|_s^{-} + \lfloor I(X)/s \rfloor s$$

(через $\left| a \right|_m^{-}$ обозначается элемент множества $\mathbf{Z}_m^{-} = \left\{ -\lfloor a/2 \rfloor, \lfloor a/2 \rfloor + 1, \ldots, \lceil a/2 \rceil - 1 \right\}$, сравнимый с a по модулю m). С учетом приведенного равенства, а также формулы (7) после деления на S выражения (9) имеем

$$X/S = \left(\left| X \right|_{M_{k-1}} + M_{k-1}\rho_{k-1}(X) \right) / \left(s\,M_{k-1} \right) + \left| I(X) \right|_s^{-} / s + \lfloor I(X)/s \rfloor. \tag{10}$$

Так как $0 \leq \left| X \right|_{M_{k-1}} < M_{k-1}$; $\rho_{k-1}(X) \leq \rho \leq k-2$;

$s \geq 2(k-1)$ (см. (7)); $-0{,}5\,s \leq \left| I(X) \right|_s^{-} < 0{,}5\,s$,

то $0 \leq \left(\left| X \right|_{M_{k-1}} + M_{k-1}\rho_{k-1}(X) \right) / (s\,M_{k-1}) < (k-1)\,M_{k-1} / 2(k-1)\,M_{k-1}) = 0{,}5$

и $-0{,}5 \leq \left| I(X) \right|_s^{-} / s < 0{,}5$.

Поэтому из выражения (10) следует, что для целочисленного приближения (8) к дроби X/S выполняется условие $(X/S - \lfloor I(X)/s \rfloor) \in [-0{,}5;\ 1)$.

Таким образом, теорема 2 доказана.

Как показывает (10), преобразование МИМК в ПК по методу доминирующего модуля практически сводится к вычислению в МИМСС ИИ $I(X)$ исходного числа $X = (\chi_1, \chi_2, \ldots, \chi_k)$ с помощью расчетных соотношений (4)–(6).

Пример 2. Пусть в МИМСС с основными модулями m_1=2, m_2=3, m_3=11 и вспомогательным модулем m_0=5 необходимо выполнить операцию масштабирования над числом $X=(1,2,7)$ с масштабом $S=M_{k-1}=M_2=6$. Согласно примеру 1 $I(X)=4$. Применяя (8) с учетом $s=1$, заключаем, что искомым целочисленным приближением к дроби $x=X/6$ служит целое число $\hat{X}=I(X)=4$. Как показано в примере 1, $X=29$. Следовательно, абсолютная погрешность указанного приближения удовлетворяет неравенству $|x-\hat{X}| = |(29/6)-4|<1$. Это полностью согласуется с теоремой 2.

Согласно условию $m_k \geq 2m_0+k-2$ для вспомогательного модуля при $m_k = 2^{b_k}$ верна оценка $m_0 \leq \lfloor (m_k-k+2)/2 \rfloor = 2^{b_k-1}+1+\lfloor -k/2 \rfloor$. Заметим, что компьютерная реализация (4), а значит, и (8) упрощается, если выполняется неравенство

$$m_k - m_0 - \rho \geq m_k - m_0 - k + 2 \geq m_k / 2. \qquad (11)$$

В этом случае ввиду $m_k = 2^{b_k}$ вычет $\hat{I}_k(X)$, вычисляемый по формуле (5), представляет собой не что иное, как b_k – битовый дополнительный код ИИ $I(X)$ и, следовательно, он непосредственно может использоваться в (9) (вместо прямого кода числа $I(X)$). В соответствии с (11) корректность обозначенного режима вычислений обеспечивается при

$$m_0 \leq 0{,}5\, m_k - k + 2 = 2^{b_k-1} - k + 2.$$

Дальнейшее упрощение операции (8) достигается при использовании множителя $s \geq 2(k-1)$ (см. (7)), который является двоичной экспонентой. Это позволяет заменить операцию деления на $(\log_2 s)$ – битовый сдвиг вправо двоичного кода компьютерного ИИ $\hat{I}_k(X)$.

Таким образом, метод доминирующего модуля позволяет осуществить преобразование с масштабированием минимально избыточного модулярного кода в позиционный код за время $(k-1)\, t_{сум} + t_{ум} + t_{сд}$, где $t_{сум}$, $t_{ум}$ и $t_{сд}$ – времена выполнения соответственно операций сложения, умножения и сдвига. При этом необходимые затраты практически сводятся лишь к одномерным таблицам ИИ.

3. Четырехмодульная СМОИ для высокоточных вычислений

Состав алгоритмического обеспечения РМВ-СМОИ и модификации его компонентов в значительной мере зависят от конкретных приложений.

Ниже рассматривается (с учетом отмеченного прикладного аспекта) основанная на вышеизложенных концептуальных положениях (см. теоремы 1 и 2) методология построения РМВ-СМОИ исследуемого класса на примере четырехмодульной системы.

Семейство вычислительных процессов, реализуемых описываемой системой, укладывается в аддитивно-мультипликативную модель, которая имеет вид

$$X_{r,t}(l) = \sum_{n=0}^{N_{r,t,l}-1} C_{r,t,l,n}\, x_{r,t}(n) \quad (r = \overline{0,\, R-1};\ t = \overline{0,\, T_r-1};\ l = \overline{0, L_{r,t}-1}), \qquad (12)$$

где $\{X_{r,t}(l)\}_{l=\overline{0,L_{r,t}-1}}$ и $\{x_{r,t}(n)\}_{n=\overline{0,N_{r,t,l}-1}}$ – соответственно выходная и входная последовательности t-й элементарной (базовой) процедуры r-й стадии описываемого вычислительного процесса; $C_{r,t,l,n}$ – некоторые константы; R, T_r, $L_{r,t}$ и $N_{r,t,l}$ – натуральные числа. Входные

последовательности $\boldsymbol{x}_{r,\,t} = \{x_{r,\,t}(n)\}_{n=\overline{0,N_{r,\,t,\,l}-1}}$ формируются из элементов выходных последовательностей $\boldsymbol{X}_{s,\,t} = \{X_{s,\,t}(l)\}_{l=\overline{0,L_{s,\,t}-1}}$ ($s \in \mathbf{Z}_r$; $t \in \mathbf{Z}_{T_s}$), определяемых согласно тому или иному правилу элементарных процедур, которые относятся к шагам с нулевого по (r–1)-й при $r \neq 0$, и из элементов входной последовательности $\boldsymbol{x} = \{x(n)\}_{n=\overline{0,\,N-1}}$ (N – длина последовательности) рассматриваемой вычислительной процедуры в случае $r = 0$. Аналитически структуру и принцип формирования входных последовательностей элементарных процедур (12), в совокупности составляющих R-шаговый рекурсивный модульный процесс выделенного семейства, в общих чертах можно описать формулой

$$x_{r,\,t}(n) = \begin{cases} x(n_{t,l,n}), & \text{если } r = 0, \\ X_{s,t_r,s}(l_{s,t_r,s,l,n}), & \text{если } r \neq 0, \end{cases} \tag{13}$$

где $\{n_{t,\,l,\,n}\}_{n=\overline{0,\,N_{0,\,t,\,l}-1}}$ – подмножество элементов кольца $\mathbf{Z}_N$, $s \in \mathbf{Z}_r$, $t_{r,s} \in \mathbf{Z}_{T_s}$, конкретный вид отображения $s \to t_{r,s}$ зависит от значений параметров r, t и l;

$\{\forall\, l_{s,\,t_{r,\,s},\,l,\,n} \in \mathbf{Z}_{L_{s,\,t_{r,\,s}}} \mid n \in \mathbf{Z}_{N_{s,\,t_{r,\,s},\,l}};\ t_{r,\,s} \in \mathbf{Z}_{T_s};\ s \in \mathbf{Z}_r\} = \mathbf{Z}_{N_{r,\,t,\,l}}$.

Выходная последовательность $\boldsymbol{X} = \{X(l)\}_{l=\overline{0,L-1}}$ (L – натуральное число) исходной вычислительной процедуры составляется из элементов выходных последовательностей $\boldsymbol{X}_{R-1,\,t} = \{X_{R-1,\,t\,(l)}\}_{l=\overline{0,\,L_{R-1,\,t}-1}}$ базовых процедур заключительного (R–1)-го шага реализуемого процесса; при этом, естественно, имеет место равенство $\sum_{t=0}^{T_{R-1}-1} L_{R-1,\,t} = L$.

Элементы подлежащей преобразованию последовательности $\boldsymbol{x} = \{x(n)\}_{n=\overline{0,N-1}}$, а также фигурирующие в (1) константы $C_{r,\,t,\,l,\,n}$ в общем случае будем считать целыми комплексными числами: $x(n) = x'(n) + jx''(n)$; $C_{r,\,t,\,l,\,n} = C'_{r,\,t,\,l,\,n} + j\,C''_{r,\,t,\,l,\,n}$ ($j = \sqrt{-1}$ – мнимая единица). Предполагается, что действительные $x'(n)$ и мнимые $x''(n)$ части элементов $x(n)$ принадлежат диапазону $\hat{\boldsymbol{D}} = \mathbf{Z}_{2P}^{-} = \{-P, -P+1, \ldots, P-1\}$ исходных данных используемой МИМСС (P – натуральное число), а действительные $C'_{r,\,t,\,l,\,n}$ и мнимые $C''_{r,\,t,\,l,\,n}$ части коэффициентов $C_{r,\,t,\,l,\,n}$ являются элементами множества $\{-Q, -Q+1, \ldots, Q\}$ (Q – натуральное число).

Поскольку при комплексных последовательностях $\boldsymbol{x}$ и коэффициентах $C_{r,\,t,\,l,\,n}$ входные и выходные последовательности элементарных процедур также комплексные:

$\boldsymbol{x}_{r,\,t} = \{x_{r,\,t}(n) = x'_{r,\,t}(n) + x''_{r,\,t}(n)\}_{n=\overline{0,N_{r,\,t,\,l}-1}}$; $\boldsymbol{X}_{r,\,t} = \{X_{r,\,t}(l) = X'_{r,\,t}(l) + jX''_{r,\,t}(l)\}_{l=\overline{0,L_{r,\,t}-1}}$,

то (13) целесообразно переписать в виде

$$\begin{cases} X'_{r,\,t}(l) = \sum\limits_{n=0}^{N_{r,\,t,\,l}-1} \left(C'_{r,\,t,\,l,\,n}\, x'_{r,\,t}(n) - C''_{r,\,t,\,l,\,n}\, x''_{r,\,t}(n)\right), \\ X''_{r,\,t}(l) = \sum\limits_{n=0}^{N_{r,\,t,\,l}-1} \left(C''_{r,\,t,\,l,\,n}\, x'_{r,\,t}(n) + C'_{r,\,t,\,l,\,n}\, x''_{r,\,t}(n)\right) \end{cases} \tag{14}$$

$$(r = \overline{0,\ R-1};\ t = \overline{0,\ T_r-1};\ l = \overline{0,\ L_{r,\,t}-1}).$$

Компьютерная реализация описанного семейства вычислительных процессов с применением мультипроцессорной технологии модулярной обработки информации предполагает декомпозицию аддитивно-мультипликативной формы (14) на k независимых модульных субпроцессов:

$$\begin{cases} X'_{r,t,l\,|\,i} = \left| \sum\limits_{n=0}^{N_{r,\,t,\,l}-1} \left(\chi'_{r,\,t,\,l,\,n,0\,|\,i} - \chi''_{r,\,t,\,l,n,1\,|\,i} \right) \right|_{m_i}; \\ X''_{r,t,l\,|\,i} = \left| \sum\limits_{n=0}^{N_{r,\,t,\,l}-1} \left(\chi'_{r,\,t,\,l,\,n,1\,|\,i} + \chi''_{r,\,t,\,l,n,0\,|\,i} \right) \right|_{m_i} \end{cases} \tag{15}$$

$$(r = \overline{0,\ R-1};\ t = \overline{0,\ T_r-1};\ l = \overline{0,\ L_{r,\,t}-1};\ i=\overline{1,k}),$$

где $X'_{r,t,l|i} = \left| X'_{r,\,t}(l) \right|_{m_i}$; $X''_{r,t,l|i} = \left| X''_{r,\,t}(l) \right|_{m_i}$;

$\chi'_{r,t,l,n,0\,|\,i} = \left| C'_{r,\,t,\,l,\,n}\ \chi'_{r,\,t,n\,|\,i} \right|_{m_i}$; $\chi''_{r,t,l,n,1\,|\,i} = \left| C''_{r,\,t,\,l,\,n}\ \chi''_{r,\,t,n\,|\,i} \right|_{m_i}$;

$\chi'_{r,t,l,n,1\,|\,i} = \left| C''_{r,\,t,\,l,\,n}\ \chi'_{r,\,t,n\,|\,i} \right|_{m_i}$; $\chi''_{r,t,l,n,0\,|\,i} = \left| C'_{r,\,t,\,l,\,n}\ \chi''_{r,\,t,n\,|\,i} \right|_{m_i}$; $\chi'_{r,t,\,n\,|\,i} = \left| x'_{r,\,t}(n) \right|_{m_i}$;

$\chi''_{r,t,\,n\,|\,i} = \left| x''_{r,\,t}(n) \right|_{m_i}$.

Субпроцесс (15) по модулю m_i выполняется независимо от других субпроцессов на отдельном процессоре СМОИ, причем в РМВ.

Из вышеприведенного описания аддитивно-мультипликативной модели вычислительных процедур алгоритмического ядра СМОИ рассматриваемого класса следует, что корректность применения РМВ обеспечивают МИМСС, удовлетворяющие теореме.

Теорема 3. *Пусть* $N_{R-r} = \max\limits_{t,\,l}\{N_{r,\,t,\,l}\}$ $(r = \overline{0, R-1})$. *Тогда динамический диапазон* $\boldsymbol{D}$ *МИМСС с основными модулями* $m_1, m_2, \ldots, m_{k-1}, m_k \geq 2m_0$, *и вспомогательным модулем* $m_0 \geq \rho$ *включает любые возможные значения величин* $X'_{R-1,\,t}(l)$ *и* $X''_{R-1,\,t}(l)$ $(l = \overline{0, L_{R-1,\,t}-1};$ $t = \overline{0, T_{R-1}-1})$, *что обеспечивает корректность РМВ, если*

$$M > P(2Q)^R \prod_{r=1}^{R} N_r, \tag{16}$$

где P *и* Q *– полумощности соответственно диапазона* $\hat{\boldsymbol{D}}$ *исходных данных и диапазона* $\{-Q, -Q+1, \ldots, Q\}$ *используемых констант*.

Модель (15) рассматриваемого семейства вычислительных процессов требует последовательного выполнения лишь трех принципиально различных с точки зрения модулярной арифметики этапов:

– преобразования элементов входной последовательности $\boldsymbol{x}$ из позиционного кода в минимально избыточный модулярный код;

– реализации помодульных компонентов вычислительного процесса;

– перевода элементов выходной последовательности $\boldsymbol{X}$ из МИМСС в позиционную систему счисления.

Пусть $P=2^{15}$, $Q=2^{12}$, $R=3$, $\prod_{r=1}^{R} N_r < 2^{10}$. Тогда согласно теореме 3 модули базовой МИМС должны быть выбраны так, чтобы выполнялось неравенство

$$M_{k-1}(m_k-\rho) \geq 2M > 2P(2Q)^R \prod_{r=1}^{R} N_r = 2^{65}. \qquad (17)$$

Исходя из фундаментальных критериев эффективности МИМА, в основу РМВ-СМОИ исследуемого класса положены следующие реализационные принципы:

– модуль m_k ИИ выбирается равным степени числа 2;

– для получения модульных сумм типа (15) применяется так называемый табличноаккумулятивный метод, предполагающий суммирование вычетов на процессоре с формированием результирующего остатка при помощи таблицы;

– умножение цифр минимально избыточного модулярного кода на константы по модулям выполняется посредством двухмерных таблиц с использованием на входах вместо значений констант их порядковых номеров.

В соответствии с неравенством (17) и приведенными принципами в качестве базовой выбрана МИМСС с основными модулями $m_1=2255$, $m_2=2257$, $m_3=2259$, $m_4=2^{32}$ и вспомогательным модулем $m_0=\lfloor (m_k - k + 2)/2 \rfloor = \lfloor (m_4 - 2)/2 \rfloor = 2^{31} - 1$. Динамический диапазон $\boldsymbol{D}$ данной МИМСС имеет мощность $2M=2\prod_{i=0}^{3} m_i \approx 4{,}93804 \cdot 10^{19} \in \left(2^{65};\, 2^{66}\right)$.

Выполнение в рассматриваемой СМОИ входного кодового преобразования для $X \in \hat{\boldsymbol{D}} = \left\{-2^{15}, -2^{15}+1, ..., 2^{15}-1\right\}$ осуществляется за время одного обращения к памяти согласно правилу $(\chi_1, \chi_2, \chi_3, \chi_4)$=(TBMOD1[$X$], TBMOD2[$X$], TBMOD3[$X$], X), где $\chi_i = |X|m_i$ ($i=\overline{1,4}$); TBMODj – идентификатор таблицы преобразования $X \to \chi_j$ ($j=\overline{1,3}$), которая состоит из $2P=2^{16}$ слов разрядностью $b_j = \lceil \log_2 m_j \rceil$ бит.

Что касается выходного кодового преобразования, т. е. преобразования минимально избыточного модулярного кода $(\chi_1, \chi_2, \chi_3, \chi_4)$ произвольного элемента X динамического диапазона $\boldsymbol{D}$ базовой МИМСС в дополнительный двоичный код целого числа $\hat{X} = \lceil X/S \rceil$, где через $\lceil a \rceil$ обозначается некоторое целочисленное приближение к величине a, то оно может быть выполнено с помощью процедуры, которая основана на теореме 2 с применением масштаба S вида (12). Однако учет специфики реализуемых вычислительных процессов позволяет выбрать для рассматриваемой РМВ-СМОИ более оптимальный масштаб: $S=Q^R = 2^{36}$.

Используя ИМФ (2) числа X:

$$X = \sum_{i=1}^{k-1} M_{i,\,k-1} \left| M_{i,\,k-1}^{-1} \chi_i \right|_{m_i} + M_{k-1} I(X) = M_{1,\,3} \left| M_{1,\,3}^{-1} \chi_1 \right|_{m_1} +$$

$$+ M_{2,\,3} \left| M_{2,\,3}^{-1} \chi_2 \right|_{m_2} + M_{3,\,3} \left| M_{3,\,3}^{-1} \chi_3 \right|_{m_3} + M_3 I(X), \qquad (18)$$

можно записать

$$\hat{X} \approx \lceil 2^{-36} \sum_{i=1}^{3} M_{i,\,3} \left| M_{i,\,3}^{-1} \chi_i \right|_{m_i} + 2^{-36} M_3 I(X) \rceil. \qquad (19)$$

Так как $0 \le 2^{-36}\sum_{i=1}^{3} M_{i,3}\,|\,M_{i,3}^{-1}\chi_i\,|_{m_i} \le 2^{-36}\sum_{i=1}^{3} M_{i,3}(m_i-1) = (2254\cdot2257\cdot2259+$ $+2255\cdot2256\cdot2259 + 2255\cdot2257\cdot2258) / 2^{36} < 0{,}5017$, то, пренебрегая в (19) величиной $\Gamma(X) = 2^{-36}\sum_{i=1}^{3} M_{i,3}\,|\,M_{i,3}^{-1}\chi_i\,|_{m_i}$ ввиду ее малости, для $\hat{X}$ получим следующее приближенное равенство

$$\hat{X} = \left\lceil \frac{M_3}{2^{36}} I(X) \right\rceil (M_3 = m_1 m_2 m_3 = 11497259565). \tag{20}$$

Применим для целочисленной аппроксимации вещественных величин правило округления. Тогда (20) примет вид

$$\hat{X} \approx \lfloor 0{,}1673071465484\, I(X) \rfloor. \tag{21}$$

Таким образом, при выбранной системе модулей преобразование минимально избыточного модулярного кода в позиционный код практически сводится к вычислению в МИМСС ИИ $I(X)$ исходного числа $X = (\chi_1, \chi_2, \chi_3, \chi_4)$.

Согласно (4)–(6) имеем

$$I(X) = \begin{cases} \hat{I}_4(X), & \text{если } \hat{I}_4(X) < 2^{31}-1, \\ \hat{I}_4(X) - 2^{32}, & \text{если } \hat{I}_4(X) \ge 2^{31}-1; \end{cases} \tag{22}$$

$$\hat{I}_4(X) = |\,I(X)\,|_{m_4} = |\,I(X)\,|_{2^{32}} = \left| \sum_{i=1}^{4} R_{1,4}(\chi_i) \right|_{2^{32}}, \tag{23}$$

где

$$R_{1,4}(\chi_1) = \left| -m_1^{-1}\,|M_{1,3}^{-1}\chi_1\,|_{m_1} \right|_{m_4} =$$

$$= \left| |-2255^{-1}|_{2^{32}} \left| |(2257\cdot2259)^{-1}|_{2255}\,\chi_1 \right|_{2255} \right|_{2^{32}} =$$

$$= \left| 487588305\,|\,282\chi_1\,|_{2255} \right|_{2^{32}}; \tag{24}$$

$$R_{2,4}(\chi_2) = \left| -m_2^{-1}\,|M_{2,3}^{-1}\chi_2\,|_{m_2} \right|_{m_4} =$$

$$= \left| |-2257^{-1}|_{2^{32}} \left| |(2255\cdot2259)^{-1}|_{2257}\,\chi_2 \right|_{2257} \right|_{2^{32}} =$$

$$= \left| 2001907663\,|\,564\chi_2\,|_{2257} \right|_{2^{32}}; \tag{25}$$

$$R_{3,4}(\chi_3) = \left| -m_3^{-1}\,|M_{3,3}^{-1}\chi_3\,|_{m_3} \right|_{m_4} =$$

$$= \left| |-2259^{-1}|_{2^{32}} \left| |(2259\cdot2257)^{-1}|_{2259}\,\chi_3 \right|_{2259} \right|_{2^{32}} =$$

$$= \left| 1621782693\,|\,1412\chi_3\,|_{2259} \right|_{2^{32}}; \tag{26}$$

$$R_{4,4}(\chi_4) = \left| M_3^{-1}\chi_4 \right|_{m_4} = \left| |(2255\cdot2257\cdot2259)^{-1}|_{2^{32}}\,\chi_4 \right|_{2^{32}} =$$

$$= \left| -300065371\chi_4 \right|_{2^{32}}. \qquad (27)$$

Следовательно, благодаря $m_4 = 2^{32}$ расчетное соотношение (21) можно записать в виде

$$\hat{X} = \begin{cases} -359289362, & \text{если } \hat{I}_4(X) = 2^{31} - 1, \\ ]0{,}1673071465484\,\hat{I}_4(X)\,[& \text{в остальных случаях.} \end{cases} \qquad (28)$$

При отказе от округлений до целых с целью повышения точности конечных результатов преобразования вместо (28) будем использовать соотношение

$$\hat{x} = \begin{cases} -359289361{,}5736, & \text{если } \hat{I}_4(X) = 2^{31} - 1, \\ 0{,}1673071465484\,\hat{I}_4(X) & \text{в остальных случаях.} \end{cases} \qquad (29)$$

Для получения слагаемых $R_{i,4}(\chi_i)$ ($i = \overline{1, 3}$) модульной суммы (23) воспользуемся одномерными таблицами ТИ1, ТИ2, ТИ3, которые в соответствии с (24)–(26) формируются по правилам

$$\text{ТИ1}[\chi_1] = |487588305\,|\,282\chi_1|_{2255}\,|\,2^{32}; \qquad (30)$$

$$\text{ТИ2}[\chi_2] = |2001907663\,|\,564\chi_2|_{2257}\,|\,2^{32}; \qquad (31)$$

$$\text{ТИ3}[\chi_3] = |1621782693\,|\,1412\chi_3|_{2259}\,|\,2^{32}, \qquad (32)$$

где переменные χ_1, χ_2 и χ_3 пробегают все значения соответственно из множеств $\mathbf{Z}_{2255}$, $\mathbf{Z}_{2257}$ и $\mathbf{Z}_{2259}$. Как следует из (30)–(32), емкость таблицы ТИi – m_i слов разрядностью 32 бита ($i = \overline{1, 3}$).

Что касается слагаемого $R_{4,4}(\chi_4)$ (см. (27)) суммы (23), то его получение табличным способом из-за большой величины модуля $m_4 = 2^{32}$ невозможно, однако в ПВМ $R_{4,4}(\chi_4)$ легко и быстро определяется путем обычного умножения (непосредственно на процессоре) цифры χ_4 преобразуемого минимально избыточного модулярного кода на целочисленную постоянную – 300065371.

Описанная МИМА-СМОИ ориентирована на четырехпроцессорную программную реализацию с повышенной точностью любых вычислительных процедур, укладывающихся в аддитивно-мультипликативную модель (15). Это, в частности, относится к таким трудоемким процедурам цифровой обработки сигналов, как алгоритмы фильтрации [2, 17], включая рекурсивную, дискретного преобразования Фурье [9] и т. п. Высокая вычислительная точность достигается за счет использования динамического диапазона большой мощности (2^{65} элементов) и расширения благодаря применению многокаскадной модели и пределов действия РМВ, характеризующегося отсутствием округлений. Это приводит также к существенному повышению производительности. Что касается известных модулярных реализаций как алгоритмов цифровой обработки сигналов [18, 19], так и других трудоемких вычислительных процедур [20], то они используют диапазоны с мощностью, не превышающей 2^{44} элементов, и ограничиваются применением однокаскадной вычислительной схемы.

Заключение

Основные результаты представленных в настоящей статье разработок по проблематике создания высокоточных СМОИ на базе МИМА состоят в следующем:

1. Для синтеза немодульных процедур, ориентированных на применение в РМВ, и, в частности, процедуры преобразования с масштабированием минимального избыточного мо-

дулярного кода в позиционный код разработана методология, которая основана на методе доминирующего модуля. Благодаря минимально избыточному модулярному кодированию элементов динамического диапазона использование данным методом ИИ в качестве базовой ИХ модулярного кода позволяет уменьшить сложность выходного кодового преобразования до $O(k)$ таблиц.

2. Описана четырехмодульная МИМА-СМОИ, полностью функционирующая в РМВ в динамическом диапазоне с мощностью, превышающей 2^{65} элементов. При этом мощности диапазонов исходных данных и констант составляют соответственно 2^{16} и 2^{12} элементов. Базовая МИМСС имеет модули 2255, 2257, 2259, 2^{32}. Созданная СМОИ адаптирована к высокоточным реализациям процедур цифровой обработки сигналов, таких, в частности, как процедуры цифровой фильтрации и дискретного преобразования Фурье.

3. На примере четырехмодульной РМВ-СМОИ показано, что учет конфигурации используемой модели вычислительных процессов в разработанной методологии синтеза немодульных процедур является эффективным средством их оптимизации. В частности, выполнение выходного кодового преобразования с масштабом, который выбирается в соответствии с порядком рекурсивности базовой аддитивно-мультипликативной модели, существенно повышает точность преобразования.

Изложенные в статье разработки проведены в рамках ГКПНИ «Инфотех».

Список литературы

1. Высокоскоростные методы и системы цифровой обработки информации / А.Ф. Чернявский [и др.]. – Минск: Университетское, 1996. – 376 с.

2. Василевич, Л.Н. Высокоскоростная модулярная реализация адаптивных цифровых фильтров с конечной импульсной характеристикой / Л.Н. Василевич, А.А. Коляда, В.В. Ревинский // Весці НАН Беларусі. Сер. фіз.-мат. навук. – 1997. – № 1. – С. 126–131.

3. Aichholzer, O. Pipeline hogenauer CIC filters using field-programmable logic and residue number system / O.Aichholzer, H. Hassler // Int. Conf. and Acoust., Speech and Signal Processing. – Seattle, 1998. – Vol. 5. – P. 3085–3088.

4. Hiasat, A.A. New efficient structure for a modular multiplier for RNS / A.A. Hiasat // IEEE Trans. Comput. – 2000. – Vol. 49, № 2. – P. 170–174.

5. Alia, G. Fast modular exponentiation of large number with large exponents / G. Alia, E. Martinelli // J. Syst. Archit. – 2002. – Vol. 47, № 14–15. – P. 1079–1088.

6. Инютин, С.А. Модулярные вычисления в сверхбольших компьютерных диапазонах / С.А. Инютин // Изв. вузов. Электроника. – 2001. – № 6. – С. 65–73.

7. Lee, K.-J. Systolic multiplier for Montgomery's algorithm / K.-J. Lee, K.-J. Yoo // Integration. – 2002. – Vol. 32, № 1–2. – P. 99–109.

8. RSA speedup with residue number system immune against hardware fault cryptanalysis / S.-M. Yen [et al.] // Lect. Notes Comput. Sci. – 2002. – Vol. 2288. – P. 297–413.

9. Мультипроцессорная реализация алгоритма Винограда для ДПФ на основе минимально избыточной модулярной арифметики / А.Ф. Чернявский [и др.] // Информатика. – 2005. – № 4. – С. 78–86.

10. Коляда, А.А. Мультипроцессорная технология модулярных вычислений / А.А. Коляда, А.Ф. Чернявский // Доклады НАН Беларуси. – 2006. – Т. 50, № 1. – С. 27–33.

11. Коляда, А.А. Мультипроцессорная технология модулярных вычислений / А.А. Коляда, Н.А. Коляда, А.Ф. Чернявский // Тр. Юбилейной Международной науч.-техн. конф. «50 лет модулярной арифметике», Москва, Зеленоград, 23–25 ноября 2005. – Зеленоград: Изд-во МИЭТ, 2006. – С. 218–231.

12. Ирхин, В.П. Табличная реализация цифровых фильтров в модулярной арифметике / В.П. Ирхин, Л.А. Овчаренко // Информационные технологии. – 2005. – № 10. – С. 13–20.

13. Модулярные параллельные вычислительные структуры нейропроцессорных систем / Н.И. Червяков [и др.] – Ставрополь: Физматлит, 2003. – 288 с.

14. Fast Modular Network Implementation for support vector machines / G.-B. Huang [et al.] // IEEE Trans. Neural Networks. – 2005. – Vol. 16, № 6. – P. 1651–1663.

15. Коляда А.А.. Модулярные структуры конвейерной обработки цифровой информации / А.А. Коляда, И.Т. Пак. – Минск: Университетское, 1992. – 256 с.

16. Евдокимов, А.А. Метод и алгоритм масштабирования для многомашинных и мультипроцессорных систем модулярной обработки информации / А.А. Евдокимов, А.А. Коляда, В.В. Ревинский // Весці НАН Беларусі. Сер. фіз.-тэхн. навук. – 2006. – № 1. – С. 104–111.

17. Мультипроцессорные вычислительные МИМА-модели для высокоточной цифровой обработки сигналов / А.А. Коляда [и др.] // Электроника инфо. – 2007. – № 11. – С. 58–62.

18. RNS-FPL nerget architectures for orthogonal DWT / J. Ramirez [et al.] // Electron. Lett. – 2000. – Vol. 36, № 4. – P. 1198–1199.

19. Овчаренко, Л.А. Повышение быстродействия цифрового фильтра в модулярной системе счисления / Л.А. Овчаренко, В.Е. Дидрих // Радиосистемы. – 2002. – Вып. 95. – № 5. – С. 43–49.

20. Маркова, В.П. Применение модулярной арифметики для моделирования диффузии / В.П. Маркова // Автометрия. – 2003. – Т. 39, № 3. – С. 60–71.

Поступила 19.07.07

Институт прикладных физических проблем
им. А.Н. Севченко БГУ,
Минск, Курчатова, 7
e-mail: razan@tut.by

A.A. Kolyada, V.V. Revinsky, A.F. Chernyavsky, H.V. Shabinskaya

FOUR MODULES SYSTEM FOR INFORMATION PROCESSING WITH PRECISE CALCULATIONS

A new approach to the organization of parallel calculations in application of minimally redundant arithmetic on program level is offered. On the basis of dominating module method the technology of synthesis of nonmodular procedures is developed. Its advantages are shown by the example of four modules system which is adapted to digital signal processing applications.